PCT/JP2004/000176

日本国特許庁
JAPAN PATENT OFFICE

JP04/176

14.1.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月１４日

出願番号
Application Number: 特願２００３－００６１７５

[ST. 10/C]: ［ＪＰ２００３－００６１７５］

出願人
Applicant(s): 松下電器産業株式会社

２００４年　２月１３日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３００８９６２

【書類名】　特許願

【整理番号】　2900655302

【特記事項】　特許法第３６条の２第１項の規定による特許出願

【あて先】　特許庁長官殿

【国際特許分類】　G06F 13/00

H04L 12/46

H04L 12/28

H04L 12/66

【発明者】

【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０４－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内

【氏名】　ペク　ユー・タン

【発明者】

【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０４－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内

【氏名】　ホン　チェン

【発明者】

【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０４－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内

【氏名】　チー　ビン・タン

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100093067

【弁理士】

【氏名又は名称】　二瓶　正敬

【手数料の表示】

【予納台帳番号】　039103

【納付金額】　35,000円

【提出物件の目録】

【物件名】　外国語明細書　1

【物件名】　外国語図面　1

【物件名】　外国語要約書　1

【包括委任状番号】　0003222

【プルーフの要否】　要

【書類名】　外国語明細書

1　Title of the Invention

A method for service and address management in WLAN inter-working

2　Claims

1. A system for managing address allocation of a mobile terminal in W LAN interworking comprising:

i. means for performing address management without requiring local resource access by using an end-to-end access control framework for sign alling;

ii. means for protecting an address management information by encry pting an end-to-end message with keys derived from authentication proced ure;

iii. means for locating a destination of the end-to-end message by using a domain information of the mobile terminal; and

iv. means for allocating address based on service requirements at a server handling a service authorization.

2. The system for managing the address allocation of the mobile termi nal in the WLAN interworking according to claim 1, wherein the system ca n realize a method of managing address allocation of the mobile terminal in WLAN interworking comprising the steps of sending address allocation requests together with an end-to-end service authorization requests fro m the mobile terminal to an authorizer in a mobile terminal's home domai n that has access to an user subscription information, allocating addres s by the authorizer in the terminal's home domain based on the service r equested and the subscription information of the user, and sending addre ss allocation reply together with the end-to-end service authorization r

eply back to the mobile terminal from the authorizer, further comprising :

i. means for supporting stateless address configuration by using wi ldcard value in the address allocation request and reply;

ii. means for supporting address type negotiation of multiple stack terminals by including a address type list in the address allocation re quest; and

iii. means for supporting allocation of multiple address for the mo bile terminal by using address prefix in the reply message, whereby it a llows the mobile terminal to form multiple addresses using this prefix.

3. The system for managing the address allocation of the mobile termi nal in the WLAN interworking according to claim 1, wherein the system ca n realize a method of managing address allocation of the mobile terminal in WLAN interworking comprising the steps of sending address allocation requests together with an end-to-end service authorization requests fro m the mobile terminal to an authorizer in a mobile terminal's home domai n that has access to an user subscription information, allocating addres s by the authorizer in the terminal's home domain based on the service r equested and the subscription information of the user, and sending addre ss allocation reply together with the end-to-end service authorization r eply back to the mobile terminal from the authorizer, further comprising :

i. means for the mobile terminal's requesting specific address by i ncluding the address requested in the address allocation request sent to the authorizer; and

ii. means for reducing service interruption by allocating same addr ess setting to the same service session at the mobile terminal.

4. The system for managing the address allocation of the mobile terminal according to claim 3 that ensures the same address setting used for the same service session further comprising:

i. an apparatus at the mobile terminal for generating session identifier that uniquely identifies the service session;

ii. means for identifying the service session of the request by including the session identifier in every service request sent to the authorizer;

iii. an apparatus at the authorizer that maintains a local database of the address settings indexed by the terminal identifier and session identifier; and

iv. means for setting the same address by retrieving settings from the local database and sending as reply to the mobile terminal.

5. The system for managing the address allocation of the mobile terminal according to claim 4 further comprising an apparatus at the authorizer that use a backend server for storing and maintaining the address setting information

6. The system for managing the address allocation of the mobile terminal in the WLAN interworking according to claim 1 that allows multiple parallel service access, wherein the system can realize a method of managing address allocation of the mobile terminal in WLAN interworking comprising the steps of sending address allocation requests together with an end-to-end service authorization requests from the mobile terminal to an authorizer in a mobile terminal's home domain that has access to an user subscription information, allocating address by the authorizer in the terminal's home domain based on the service requested and the subscription information of the user, and sending address allocation reply togethe

r with the end-to-end service authorization reply back to the mobile ter minal from the authorizer, further comprising:

i. means for requesting multiple services in one request message by grouping service request and address request for each service, and aggr egating multiple groups in one request message;

ii. means for the authorizer's negotiating multiple service setting by sending multiple negotiation message independently to different netw orks that provide the services; and

iii. means for configuring the mobile terminal with the multiple se rvice settings by aggregating the multiple service and address setting i nformation groups into one reply message.

7. The system for managing the address at the mobile terminal that al lows the multiple parallel service accesses with different address setti ngs in the WLAN interworking according to claim 6 further comprising:

i. an apparatus that maintains a local database of a service sessio n information with corresponding address settings in the mobile terminal ; and

ii. means for using different addresses for different service sessi ons at the mobile terminal by multiplexing the address settings using a session identifier.

8. A system for managing a tunnel settings of a mobile terminal in WL AN interworking comprising:

i. means for performing tunnel management without requiring local r esource access by using an end-to-end access control framework for signa lling;

ii. means for protecting a tunnel management information by encrypt ing an end-to-end message with keys derived from authentication procedur

e; and

iii. means for setting up tunnels according to service requirements at the server handling a service authorization.

9. The system for managing the tunnel settings of the mobile terminal in the WLAN interworking according to claim 8, further comprising:

i. means for negotiating the tunnels for the mobile terminal's supporting multiple tunnel types by including a tunnel type list in a tunnel request message sent by the mobile terminal; and

ii. means for negotiating tunnel directions by including a tunnel direction information in the tunnel request message sent by the mobile terminal.

10. The system for managing the address allocation and tunnel setup in the WLAN interworking according to any one of claims 1 to 9, wherein a message sequence allows configurations to be accomplished within one round message exchange, the message sequence comprising the steps of:

i. the mobile terminal's sending request contains service authorization request information, address allocation request information, and tunnel setup information to the service authorizer in its home domain;

ii. an authorizer's making service authorization decision based on an users subscription information;

iii. the authorizer's exchanging information with the network providing the requested service on a service attributes negotiation, the address allocation, and tunnel settings;

iv. the authorizer's exchanging information with the WLAN on the service attributes negotiation, the address allocation, and the tunnel settings; and

v. the authorizer's sending the consolidate information to the mobi

le terminal including the negotiated service settings, the address setti ngs, and the tunnel settings.

11. The system for managing the address allocation and the tunnel set up in the WLAN interworking according to claim 10, whirein the message s equence further comprises the step of the authorizer's contacting a back end server in the home network for the user's subscription information.

12. The system for managing the address allocation and the tunnel set up in the WLAN interworking according to claim 10 or 11, wherein a set o f message format to be used for the mobile terminal in the message seque nce comprises:

i. mobile user's home domain information accessible to all network nodes;

ii. mobile user's identity accessible only by the service authorize r;

iii. service request information that contains one or more service requests accessible only by the service authorizer;

iv. address allocation request information that contains address ty pes, and one or more specific addresses desired;

v. tunnel setting request information that contains tunnel types to be used and tunnel end points information;

vi. identifier of the WLAN that gives the location information of t he mobile terminal; and

vii. security information to protect integrity of the message.

13. The system for managing the address allocation and the tunnel set up in the WLAN interworking according to claim 10 or 11, wherein a set o f message format to be used between the authorizer and the WLAN in the m

essage sequence comprising:

i. identifier of the home network of the mobile terminal for networ k based service policy to apply on a service and address request;

ii. identifier of the mobile terminal in the service and address re quest;

iii. service request information that contains service specific att ributes for service provisioning negotiation;

iv. address allocation request information that contains address ty pes, and one or more specific addresses desired;

v. tunnel setting request information that contains the tunnel type s to be used and tunnel end points information; and

vi. security information to protect integrity of the message.

14. The system for managing the address allocation and the tunnel set up in the WLAN interworking according to claim 10 or 11, wherein a set o f message format to be used between the authorizer and the network provi ding the requested service in the message sequence comprising:

i. identifier of a home network of the mobile terminal for network based service policy to apply on a service and address request;

ii. identifier of a service session regarding this service request;

iii. identifier of the mobile terminal in the service and address r equest;

iv. service request information that contains service specific attr ibutes for service provisioning negotiation;

v. address allocation request information that contains address typ es and one or more specific addresses desired;

vi. tunnel setting request information that contains the tunnel typ es to be used and tunnel end points information; and

vii. security information to protect integrity of the message.

15. The system for managing the address allocation and tunnel setup i n the WLAN interworking according to any one of claims 1 to 9 further co mprising:

i. means for modifying a QoS settings, filtering settings to reduce s ervice interruption by using a policy control framework to signal corres ponding control nodes; and

ii. means for using the policy control framework by setting an interf ace between a service authorizer and a policy server.

16. The system for managing the address allocation and the tunnel set up in the WLAN interworking according to claim 15, wherein a set of mess age format used for information exchange between the service authorizer and the policy server comprises:

i. operation identifier that indicates an operation to be taken by th e policy server;

ii. identifier of the mobile terminal;

iii. location information of the mobile terminal for applying locatio n based policy to the mobile terminal;

iv. service type and session information of a corresponding request;

v. tunnel setting used by the mobile terminal for accessing the servi ce; and

vi. address information of the mobile terminal for accessing the serv ice.

17. A method of managing address allocation of a mobile terminal in W LAN interworking comprising the steps of:

i. sending address allocation requests together with an end-to-end service authorization requests from the mobile terminal to an authorizer

in a mobile terminal's home domain that has access to an user subscription information;

ii. allocating address by the authorizer in the terminal's home domain based on the service requested and the subscription information of the user; and

iii. sending address allocation reply together with an end-to-end service authorization reply back to the mobile terminal from the authorizer.

18. The method for the mobile terminal address management in the WLAN interworking according to claim 17, further comprising the steps of:

i. negotiating the address to be allocated to the mobile terminal between an address management entity in a network that provides the service requested by the mobile terminal and an authorizer in the mobile terminal's home domain; and

ii. negotiating the address allocation between an address management entity in the WLAN where the mobile terminal is present and the authorizer in the mobile terminal's home domain.

19. A method for maintaining the address settings at the authorizer which identifies the service session request of a mobile terminal by including the session identifier, maintains a local database of address settings indexed by a terminal identifier and a session identifier and sets the same address by retrieving settings from the local database, comprising the steps of:

i. creating a new entry with the terminal identifier and the session identifier which the authorizer receives from the mobile terminal as the index when such entry could not be found in the local database;

ii. storing the created entry into the database after successfully

allocated the address for the mobile terminal; and

iii. deleting the stored entry from the database when the mobile te rminal requested to terminate the corresponding service session.

20. A method for setting up client based tunnel for a mobile terminal in the WLAN interworking in the system which comprises means for perfor ming tunnel management without requiring local resource access by using an end-to-end access control framework for signalling, means for protect ing a tunnel management information by encrypting an end-to-end message with keys derived from authentication procedure, and means for setting u p tunnels according to service requirements at the server handling a ser vice authorization, comprising the steps of:

i. sending tunnel requests together with an end-to-end service auth orization requests from the mobile terminal to the authorizer in the mob ile terminal's home domain that has access to an user subscription infor mation with a tunnel type set to client based and client address informa tion;

ii. allocating address to be used for the tunnel by the authorizer in the mobile terminal's home domain based on the service requested and the subscription information of the user;

iii. informing the other end point of the tunnel of corresponding i nformation by the authorizer; and

iv. sending client tunnel setting information together with an end- to-end service authorization reply back to the mobile terminal from the authorizer.

21. The method for setting up client based tunnel for the mobile term inal in the WLAN interworking according to claim 20 further comprising t he steps of:

i. the authorizer's contacting the WLAN for allocating of WLAN local address to be used for setting up the tunnel; and

ii. the authorizer's contacting the WLAN for setting up a routing or filtering setting to allow the tunnel pass through.

22. A method for setting up network based tunnel for a mobile terminal in the WLAN interworking in the system which comprises means for performing tunnel management without requiring local resource access by using an end-to-end access control framework for signalling, means for protecting a tunnel management information by encrypting an end-to-end message with keys derived from authentication procedure, and means for setting up tunnels according to service, requirements at the server handling a service authorization, comprising the steps of:

i. the terminal's sending a tunnel setup request together with an end-to-end service authorization request to the authorizer in the mobile terminal's home domain that has access to an user subscription information with a tunnel type set to network based together with a terminal local identifier;

ii. the authorizer's contacting the WLAN for setting up a tunnel end points;

iii. the authorizer's contacting the network providing a service for setting up the tunnel end points; and

iv. the authorizer's replying the terminal with the address of the tunnel end points in the WLAN together with the service settings.

3 Detailed Description of Invention

Industrial Field of Utilisation

The invention pertains to the field of wireless data communication. Mo

re particularly, this invention relates to the address management in the wireless LAN environment for the mobile user who comes from other networks. It could be used for the inter-working of the WLAN to the public radio networks, e.g. 3G networks, or WLANs using other radio technologies or in another administrative domain. The invention is used by the WLAN and the inter-worked network as well as the mobile terminal, for the address allocation, configuration, tunnelling set-up, etc, so that the mobile terminal is able to access services it subscribed to in the WLAN.

Background and Prior Art

In WLAN inter-working, the terminal needs to be addressable so that it can access any service it subscribed to. When the services are delivered over IP, the terminal must be attached to certain IP address. In the mobile world, the point of attachment of the terminal changes frequently. It is highly possible that the terminal traverses a few domains during one active service session. To satisfy the requirements of terminal mobility, the address management mechanism is needed to configure and update the terminal's address every time it changes the point of attachment.

MobileIP is an open standard, defined by the Internet Engineering Task Force (IETF) [Non-patent document 1] [Non-patent document 2], that provide a solution for the address management and traffic routing for the mobile terminals. It allows the user to remain reachable using the same address when roaming among different IP networks. Since the mobility is controlled at the IP level, it is not bound to the underlying link layer technologies. Therefore, for terminals in the 3G cellular networks, or the Wireless LAN, e.g. 802.11 networks, same protocol stack could apply. With the merging of the access technologies, e.g. the inter-working of the WLAN and 3G cellular networks, this kind of harmonized level solution is especially useful. In MobileIP, the address management is done over t

he IP connectivity. In case the IP connectivity is not available, it cou ld not work. MobileIP also requires the terminal to own a Home Address, and know its Home Agent. This might not be available in the inter-workin g scenarios, e.g. when the terminal powers up in the foreign WLAN for th e first time.

MobileIPv6 draft has introduced a way of setting the home address of t he mobile node [Non-patent document 2]. The terminal would generate a ca re of address first, e.g. utilizing DHCPv6 [Non-patent document 3], and use this address to communicate with its home network to set up the fina l home address. In WLAN inter-working, this is not workable, since the m obile node's home network may not be always reachable using the care of address obtained from the WLAN. Also, the multiple round-trip configurat ion procedure would be time consuming, and could not meet the expectatio n of the users.

The Diameter Mobile IPv6 Application [Non-patent document 4] presented a solution based on the AAA architecture for the address management for the MobileIPv6. This solution utilized the AAA servers and clients in t he visited and home network to carry out the address updating and agent discovery. The mechanism requires the mobile node to have local IP conne ctivity for the message exchange, e.g. able to listen for the Router Adv ertisement messages, and this is not always possible due to the foreign domain's local policy. Also, the scheme only caters for the situation wh ere the address belongs to the mobile terminal's home domain. In the WLA N inter-working, the terminal would use address from another domain depe nding on the service it's accessing. This could not be supported in the scheme since it has not information of the service request of the termin al. This scheme is designed for the Mobile IPv6 environment, and therefo re could not work with terminals with no Mobile IP stack.

3GPP also provided a solution, GTP [Non-patent document 5] for managin

g the terminal addressing and tunnelling. GTP comprises two parts, GTP-C for control and GTP-U for user data traffic. GTP runs over UDP, and encapsulates the user data in the UDP packets. The GTP is designed for the GPRS [Non-patent document 6] network, and therefore depends heavily on the GPRS network's features, e.g. GGSN, SGSN nodes. This makes it difficult to be deployed in the simple wireless access network, e.g. WLAN.

Disclosure of Information on prior art documents

[Non-patent document 1]

"IP mobility support for IPv4" http://www.ietf.org/rfc/rfc3344.txt

[Non-patent document 2]

"Mobility support in IPv6" http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-19.txt

[Non-patent document 3] "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" http://www.ietf.org/internet-drafts/draft-ietf-dhc-dhcpv6-28.txt

[Non-patent document 4] "Diameter Mobile IPv6 Application" http://www.ietf.org/internet-drafts/draft-le-aaa-diameter-mobileipv6-02.txt

[Non-patent document 5] "GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (Release 5)" 3GPP TS 29.060 V5.3.0 (2002-09) ftp://ftp.3gpp.org/Specs/archive/29_series/

[Non-patent document 6] "General Packet Radio Service (GPRS); Service description; Stage 2 (Release 5)" 3GPP TS 23.060 V5.2.0 (2002-06) ftp://ftp.3gpp.org/Specs/archive/23_series/

[Non-patent document 7] "IP Multimedia Subsystem (IMS); Stage 2 (Release 5)" 3GPP TS 23.228 V5.6.0 (2002-09) ftp://ftp.3gpp.org/Specs/archive/23_series/

[Non-patent document 8] "Diameter Base Protocol" http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-15.txt

[Non-patent document 9] "PPP Extensible Authentication Protocol (EAP

)"　http://www.ietf.org/rfc/rfc2284.txt

[Non-patent document 10]　3GPP project http://www.3gpp.org

[Non-patent document 11]　3GPP2 project http://www.3gpp2.org

[Non-patent document 12]　"The Network Access Identifier"　http://www.ietf.org/rfc/rfc2486.txt

[Non-patent document 13]　"Numbering, addressing and identification (Release 5)"　3GPP TS 23.003 V5.3.0 (2002-06) ftp://ftp.3gpp.org/Sepcs/archive/23_series/

[Non-patent document 14]　"Port-Based Network Access Control"　IEEE Std 802.1X-2001 http://standards.ieee.org/getieee802/

[Non-patent document 15]　"Diameter Extensible Authentication Protocol (EAP) Application"
http://www.ietf.org/internet-drafts/draft-ietf-aaa-eap-00.txt

[Non-patent document 16]　"Diameter NASREQ Application"　http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-nasreq-09.txt

[Non-patent document 17]　"IPv6 Stateless Address Autoconfiguration"
http://www.ietf.org/rfc/rfc2462.txt

Problems to be solved

Usually WLAN and the inter-worked network are in different administrative domains, which means their address spaces are managed separately. Therefore, when a mobile terminal roams into a WLAN in a different domain than its home network, some address configuration must be carried out to guarantee the continuous service delivery to the terminal. This address configuration could include for example IP address allocation, address registration, tunnelling set-up, etc.

For certain services delivered to the terminal over the WLAN, address restrictions would apply. For example, to access the IMS [Non-patent document 7] service in the 3G networks from the WLAN would require the term

inal to own an address belonging to the network providing the IMS. Consequently, a mobile terminal with parallel access to different services would be required to have multiple IP address configured.

In WLAN, terminals are not allowed to use any resources, e.g. send or receive normal data packets, before they are authenticated, and authorized to do so. Using normal schemes, e.g. the one suggested in MIPv6, the address configuration could only happen after the successful authorization procedures. This kind of approach is slow, and is not able to meet requirements of some of the services. In order to have the address configured before the authorization, relevant information needs to be integrated into the access control messages.

The address management is usually based on the user's subscription information. Therefore, it must be controlled by the mobile terminal's home network. For certain external services, the address needs to be allocated from domain other than the home network. In this case, a mechanism is required to allow the home network to negotiate the address allocation, and other information with that domain.

When a terminal changes its address, the end-to-end QoS associated to it would be affected. For example, a traffic filter based on source or destination address information would not be able to correctly classify the streams if the address changed. For a WLAN that implements firewall or other traffic control functions, the terminal's new address also needs to be signalled, otherwise traffic could be blocked or dropped.

Means for Solving the Problems

When a terminal enters a WLAN, it must go through the authentication, authorization procedures to gain access to the resources. In this invention, a solution is presented for address management that is integrated into the access control mechanisms. By this integration, the terminal's a

ddress could be configured together with the granting of access. The terminal would reuse and extend the access control mechanisms, and therefore does not need to implement any new protocol. The configuration process would be shielded by the inherent encryption and protection of the access control process, and thus need no extra security setup.

The present invention also provides means for the terminal's home network to negotiate the address management with the network that provides the service to the terminal. This kind of negotiation is a back-end process, and is transparent to the mobile terminal and WLAN. Result of the negotiation would be carried along to the WLAN and mobile terminal using the service authorization procedures.

When parallel access sessions are present to the same terminal, multiple addresses could be required. The invention provides a method for the terminal to obtain address that binds to the session, using a fine grain service authorization procedure. Each session would use the address attached to it, and transition to a new address is allowed.

The address management is also integrated with the policy control mechanisms. The policy control would provide means for the terminal and its home network to configure the WLAN when necessary after an address alternation. QoS, or tunnelling information would be modified and provisioned accordingly to the new status using channels available in the existing policy control procedures. By this, a smooth address transition in the roaming time could be achieved, and QoS interruption could be minimised.

Embodiments

The present invention is to be used for the WLAN to inter-work with other networks. The inter-worked network could be another WLAN or a public cellular network. It is easy to deploy the invention in both of the cases. The invention is to be used for the purpose of address management an

d service provisioning relevant to the address transition, i.e. mobility control.

The deployment of the proposed scheme, no extra interface and protocol implementation are necessary. The scheme would reuse the existing acces s control mechanisms, and extend some of the attributions to support the necessary functionalities. The address allocation, and modification wou ld be integrated with the service authorization procedures. Since the au thorization procedure is encrypted and protected by the credentials obta ined from the authentication, the address information is also protected with same level of security. It would be shown as part of the authorizat ion information, and could be transferred the same way as normal authori zation information. For example, it could be included in the Diameter [N on-patent document 8] as an authorization specific AVP, or an EAP [Non-p atent document 9] attribute if an EAP method for authorization is availa ble.

When a terminal enters the WLAN, it would be authenticated and authori zed before allowed to use the service. In the authorization procedure, t he terminal would request for the service it tends to access. This infor mation would be passed back to the terminal's home network by the WLAN. The terminal's home network decides whether to allow the service based o n the user's subscription profile. Depending on the service requested, t he terminal's home network also decides the address to be used for the s ervice. For example, for an IMS service, the address needs to be allocat ed from the IMS address space, whilst for a local WLAN service, the addr ess obtained locally would be sufficient. Also, tunnelling information r elated to the address management would be identified.

The address information would be included in the authorization informa tion, and sent along with the authorization success message. Part of the information is destined for the WLAN, and part for the terminal, simila

r to the normal authorization procedure. For example, the address needs to be sent to the terminal so that it can configure itself, and the tunnelling information would be used by the WLAN if network tunnelling were necessary.

When any change in address is necessary, the re-authorization procedure could be used for a quick update without going through the service authorization details.

Policy control would be triggered when the terminal starts to access the service. Address information would be made available to the policy server at the terminal's home network. The policy server could then make policy decisions based on the address information. When address changes, the policy server would be notified to update the corresponding policies, so that the QoS and service provisioning could be guaranteed.

To help understanding the invention, the following definitions are used:

A "WLAN" refers to wireless local area network. It contains arbitrary number of devices in order to provide LAN services to mobile terminals through wireless technologies.

A "3G network" refers to a 3rd generation public access network. An example could be the system defined by 3GPP [Non-patent document 10], or 3GPP2 [Non-patent document 11].

A "Mobile Terminal" refers to a device used for accessing the service provided by the WLAN and other networks through wireless technologies.

A "Home Network" refers to the network where the mobile terminal (MT)'s service subscription information stored. In the inter-working scenarios, it could be the network the MT originally subscribed to, or a visited network that is authorized to have full access to the MT's subscription information.

A "Service Provider Network" refers to the network where the service the MT requested is provided. It could be any network, e.g. the home network, the WLAN, or an external network.

A "Network Element" refers to any functioning device in the network that can carry out information processing.

A "Policy Server" refers to a network element that performs the policy control function of the network domain. The policy control function includes, for example, the local resource allocation, packet filter updating, routing updating, etc.

An "Air Interface" refers to any radio access technologies for the mobile terminal to access the WLAN.

A "stream" is a gathering of packets transferred in the network that have certain attributes in common.

A "Traffic" is a gathering of streams transferred in the network.

A "flow" refers to the data path and the network resources needed for the data path used in delivering the stream.

"QoS" refers to the term Quality of Service of a data streams or traffic.

"Message" refers to the information exchanged between the Network Elements for the purpose of Inter-working control.

"Operation Sequence" refers to a series of Message Exchange between certain Network Elements in certain order for Inter-working control.

"Upper Layer" refers to any entity on top of the current entity that process the packet passed to it from the current entity.

"Client Based Tunnel" refers to the tunnelling scheme that one of the end points of the tunnel is the Mobile Terminal.

"Network Based Tunnel" refers to the tunnelling scheme that the end points of the tunnel reside on Network Elements other than the Mobile Terminal.

In the following description, for purposes of explanation, specific numbers, times, structures, protocol names, and other parameters are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to anyone skilled in the art that the presented invention may be practiced without these specific details. In other instances, well-known components and modules are shown in block diagram in order not to obscure the present invention unnecessary.

Due to the highly mobile characteristics of the terminal, mobility control is one of the most prominent issues for WLAN inter-working. When a terminal moves, it could be forced to use an address that is not local to its point of attachment. For example, for a 3G terminal roamed into the WLAN, it needs a 3G-domain address to access its home network's service, e.g. IMS service. When the terminal initiated the service inside the 3G networks, the address is allocated according to 3G schemes, e.g. GPRS service [Non-patent document 6]. This address would be bound to the terminal's 3G cellular interface. When a terminal enters the WLAN domain, it could desire to communicate using its WLAN interface since that can provide higher throughput. For example, a PDA with dual interface, GPRS and IEEE802.11, would desire to use its GPRS interface on the road, and use its IEEE802.11 interface in the hotspot. When using the WLAN interface accessing the 3G service, the terminal needs to continue using the same address obtained from the 3G interface. Otherwise, the terminal would face service interruption, and be forced to re-initiate the session, which is not desirable to the user. Since the address in use is not local to the WLAN, a tunnel must be set up from the terminal to the Service Provider Network.

An example implementation of the invention for address allocation and tunnel set-up is shown in Figure 1. To avoid confusion, only Network Ent

ities that participate in the signaling are shown.

The Mobile Terminal (101) is the entity that requests a certain service from the network. In real world, it could comprise several entities, e.g. a handset connected to the laptop computer via a Bluetooth link. It is drawn as one set in Figure 1 for the reason of simplicity. Among the WLAN Functions (1001), the Access Point (105) is the entity that provides WLAN access to the Mobile Terminal (101). Access Point (105) would block all the data traffic from the Mobile Terminal (101) until it is authorized to use the WLAN services. A control channel that only allows certain specific data packets is left open for the access control signaling. Mobile Terminal (101) communicates with the Access Point (105) over the wireless link (1011). This link could use any kind of wireless technology, e.g. IEEE802.11, HiperLan/2, Infrared, etc. This does not preclude the use of other technologies, e.g. Optical Fiber, for this link, if similar access control technology could apply. Another entity in the WLAN is the WLAN Management Server (WLAN Server) (102). This WLAN Server (102) is in charge of the address space management, and resource management of the WLAN. It could reside on the WLAN gateway, or, in a simple WLAN, even collocate with the Access Point (105). The WLAN Server (102) communicates with Access Point (105) over interface (1015). This is for WLAN resource control and service provisioning, e.g. QoS management over air interface. To manage the WLAN, the server could interact with other entities of the WLAN, e.g. the WLAN gateway or Firewall, which is not shown in the diagram.

In the terminal's Home Network (1002), a Home Network Authorizer (103) controls the service authorization and address allocation. The Access Point (105) and WLAN Server (102) both communicates with the Home Network Authorizer (103) for service control information over the link (1012) and link (1014) respectively. Physically, the link (1012) and the link (1

014) could be identical, i.e. between same end points, using the same pr otocol, and encapsulated in the same packet, but they are logically sepa rated.

The Mobile Terminal (101) could request for any service it subscribed to. These services could be in the Home Network (1002), a separate Servi ce Provider Network (1003) or even the WLAN itself. When the service is provided by the Home Network (1002) or the WLAN, the Service Provider Ne twork (1003) would overlap with these networks, and thus the control fun ctions could bind together. The Service Provider Network Management Serv er (Service Provider Network Server) (104) controls the service authoriz ation, and address allocation in the Service Provider Network (1003). Th e Home Network Authorizer (103) communicates with it over a control inte rface (1013). In real implementation, the Service Provider Network (1003) could be the WLAN, the Home Network (1002) or another network. In case the service is provided in the Home Network (1002), this interface beco mes an internal interface, and does not need to follow the exact format and using the same protocol as described in the following example implem entation.

Figure 2 shows an example operation sequence for the address managemen t for the WLAN inter-working using the above-described framework. In the operation, it is assumed that the Mobile Terminal (101) has already fin ished the WLAN association and authentication procedure (201). This mean s that the Mobile Terminal (101) and the Access Point (105) has already mutually authenticated each other, and encryption protection has already been turned on for the following message exchanges. When the Mobile Ter minal (101) wants to access any service over the WLAN, it sends out the MT_Request_A message (202A) over the link (1011) to the Access Point (10 5), and destined to its Home Network Authorizer (103). This message is e nd-to-end protected by the keys generated from the authentication proced

ures (201). Figure 3 shows an example implementation of the message MT_Request_A Message (202A).

The message starts with the Message_Type field (301). This field identifies which kind of message is encapsulated, e.g. Request, Reply, etc. The length of this field is one octet. Message types are represented by integer numbers. This is to save the limited resources for signaling over the air interface. It is obvious to anyone skilled in the art that this field could adopt any other format when necessary. Following the Message_Type field (301) is the Message_Length field (302). It contains the information about the length of the whole message, including the Message_Type field (301). Next field is the Domain_Name field (303). This field identifies the home domain of the Mobile Terminal (101). The Network Access Identifier (NAI) [Non-patent document 12] could be used, and it would be in the form of, for example, "UserID@home.domain.3gpp.org". To protect the user identity, the UserID part before the "@" sign is using a wildcard value, e.g. "roamed". The home domain information is used for routing the message to the Mobile Terminal (101)'s Home Network Authorizer (103).

The above three fields, Message_Type field (301), Message_Length field (302), and Domain_Name field (303), are protected by the security association between the Mobile Terminal (101) and the Access Point (105). This security association is obtained from the Authentication procedure (201) for the protection of air interface. Therefore, the information contained in these fields could be accessed by the Access Point (105) for forwarding purpose. The fields following the Domain_Name field (303) would be protected by the security association between the Mobile Terminal (101) and Home Network Authorizer (103). For example, it could be public key of the Home Network Authorizer (103), or the session key derived from Authentication procedure (201). The UserID part from the Domain_Name fie

ld (303) could be used to signal the index of the keys that is used for the message protection.

After the Domain_Name field (303) is the MT_ID field (304). This field contains the information to uniquely identify the Mobile Terminal (101) in the Home Network (1002) context. This could be, for example, the IMSI [Non-patent document 13] of the Mobile Terminal (101), or the TMSI [Non-patent document 13] gained in the authentication procedures. The Home Network Authorizer (103) uses this identifier to retrieve the user's subscription information. It is obvious to anyone skilled in the art that any other format could be used in this field as long as the Home Network Authorizer (103) could map it to the actual user identity.

The next field is the Service_Request field (305). This field is used by the Mobile Terminal (101) to indicate the service it desire to access to the Home Network Authorizer (103). Since the message is between the Mobile Terminal (101) and its Home Network Authorizer (103), it is operator and network specific. For example, in a 3GPP network, this could be the APN [Non-patent document 13] that identifies the GGSN to use and the special service to access. It is obvious to anyone skilled in the art that other formats could be used if the Home Network (1002) is of another type. Other service request information could also be appended, e.g. the bandwidth request. A possible value of the field could be "2M.bandwidth.request.IMS.foo.bar.operator-name.operator-group.gprs". The part after the "request" is the standard APN to identify the service, and the part before the "request" is the specific service request. The actual request attribute is service dependent, and could be defined by the operator. The Mobile Terminal (101) could gain the knowledge of the format from the SIM or USIM card.

A Session_ID field (306) provides the session control information. This is used for the Mobile_Terminal (101) to identify the session this ser

vice request concerned to the Home Network Authorizer (103). The identif ier of the session should be locally unique within the Mobile_Terminal (101). The Mobile Terminal (101) should maintain a local record of all th e service sessions. A new entry with a new session identifier would be c reated whenever a new service session starts. The entry would be removed when the session terminates, and the identifier would be freed for reus e. In the example implementation, the field is 2 octets, and the identif ier is in hexadecimal value. It is obvious to anyone skilled in the art that other type of identifier supported by the terminal could be used. T he MT_ID field (304) and the Session_ID field (306) uniquely identify a service session at the Home Network Authorizer (103).

Address_Request field (307) contains the information about the address allocation request from the Mobile Terminal (101). In the example imple mentation, a compound structure is used, as shown in Figure 4. The first part of the structure is the Address_Type field (401). This would ident ify which type of address is supported by the Mobile Terminal (101). The size of this field is one octet. Possible value could be:

No_IP ::= 0x00;

Single_Stack_IPv4 ::= 0x01;

Single_Stack_IPv6_FullAddress ::= 0x02;

Single_Stack_IPv6_Prefix ::=0x03;

Dual_Stack_IPv4_Preferred ::= 0x04;

Dual_Stack_IPv6_Preferred_FullAddress ::= 0x05;

Dual_Stack_IPv6_Preferred_Prefix ::=0x06

It is obvious to any one skilled in the art that there could be more t ypes supported, and other numbers used. The second part of the structure is the Suggestion_Length field (402). This field indicates the length o f the following field Address_Suggestions field (403). The Address_Sugge stions field (403) lists out the address that the Mobile Terminal (101)

desires to be assigned. For example, an ongoing session is using a certa in address, it would be important to have the same address assigned to k eep the session uninterrupted. The Address_Suggestions field (403) could be a list of addresses. Each entry in the list starts with a one-octet type field stating the address type, e.g. IPv4, or IPv6, and followed by the actual address. For the Home Network Authorizer (103) that does not support the terminal address suggestion feature, the Suggestion_Length field (402) and Address_Suggestions field (403) would be silently ignore d.

After the Address_Request field (307) is the Tunnel_Request field (308). This field is used by the Mobile Terminal (101) to indicate which typ e of tunnel it supports. The first octet of the field indicates the leng th of this field, including itself. The content of this field could be a list, with each entry occupying two octets. The first octet of each ent ry contains the identifier of the tunnel type the Mobile Terminal (101) supports. The value of the octet could be:

Network Tunnel -- Generic::= 0x01;

Network Tunnel -- Mobile IPv4::=0x02;

Client Tunnel -- Generic::= 0x04

Client Tunnel -- Mobile IPv4::= 0x05;

Client Tunnel -- Mobile IPv6::= 0x06;

No Tunnel ::= 0x08

It is obvious to anyone skilled in the art that other tunnel types cou ld be defined and used in the field. The second octet of each entry indi cates the direction of the tunnel. Possible value of this octet could be :

Tunnel -- From terminal ::=0x01;

Tunnel -- To terminal ::=0x02;

Tunnel -- Bi-directional ::=0x03;

The first entry in the list indicates the Mobile Terminal (101)'s preferred type.

The next field in the MT_Request_A message (202A) is the WLAN_ID field (309). It contains the information to identify the WLAN to the Home Network Authorizer (103), so that it could make decisions based on the location, or provide location-based service to the Mobile Terminal (101). The WLAN_ID could be obtained from the authentication procedures, or from the broadcasted information from the Access Point (105), e.g. the SSID in IEEE802.11 network. A Mobile Terminal (101) local identifier is also included. This is for the Access Point (105) to identify the terminal.

The last field is the Security_Field (310). This field contains the information to protect the message. The exact algorithm used for the field is negotiated between the Mobile Terminal (101) and its Home Network Authorizer (103). This could be settled at the user subscribing time, or saved into the SIM or USIM card of the terminal. It could also be implemented as software module, and to be downloaded whenever necessary.

The fields in the MT_Request_A message (202A) may not need to follow the exact sequence as described above. For example, in real implementation, the fields (304) to (309) could be placed in any order as long as they place a field identifier in the front.

In real implementation, the message could be carried over the link (1011) using any suitable mechanism. For example, in an IEEE802.11 network, it could be implemented as an EAP message, and use the EAPOL defined in IEEE802.1x to carry [Non-patent document 14].

When the Access Point (105) received this message, it would retrieve the home domain information from the Domain_Name field (303). The Access Point (105) could obtain the Home Network Authorizer (103)'s address using the domain information, e.g. make a DNS enquiry. The Access Point (105) would forward the message to the corresponding Home Network Authorize

r (103) according to this information. In certain case, the WLAN would h ave a central AAA server, the Access Point (105) would forward the messa ge to the AAA server directly, and the WLAN AAA server would parse the d omain information, and forward the message to the actual Home Network Au thorizer (103). It is assumed that between the Access Point (105) and th e Home Network Authorizer (103), a secure link exists. This could be set up during the authentication procedure (201), or dynamically setup using the security association derived from that process.

The Access Point (105) need not participate in the message processing, and therefore need not to implement the whole stack to parse the messag e. It would only need to read the message type, and do the re-encapsulat ion, and forwarding, shown as step MT_Request_B message (202B). The prot ocol used for the forwarding could be any suitable AAA protocol, e.g. th e EAP application for Diameter [Non-patent document 15] or NASREQ applic ation for Diameter [Non-patent document 16]. Those protocols are already available on the Access Point (105) for the purpose of authentication. Therefore, the message MT_Request_A message (202A) is essentially sent e nd-to-end from Mobile_Terminal (101) to the Home Network Authorizer (103), similar to the end-to-end authentication procedure (201).

Figure 5 shows an example implementation of the Home Network Authorize r (103)'s state machine. The Home Network Authorizer (103) starts from t he Init state (501) to the Idle state (502) performing the process Initi ate() at the transition (5001). The Initiate() process includes any nece ssary steps to establish connections with other backend servers, securit y associations, etc. It is obvious to anyone skilled in the art that oth er process could be involved depending on the setting in the real implem entation.

When the Home Network Authorizer (103) received the MT_Request_B messa ge (202B) forwarded from the Access Point (105) at the transition (5002)

, it would transit to the Message Decrypt state (503). Figure 6 shows an example of the implementation of Message Decrypt state (503). In the Message Decrypt state (503), the Home Network Authorizer (103) would decrypt the fields in the MT_Request_B message (202B) using the keys identified by the Domain_Name field (303) in the step (6001). If the message is damaged, or detected modified using the Security_Field (310) in the step (6002), the Home Network Authorizer (103) would set the flag to Bad Message in the step (6013), and the state machine would transit to Service Reject state (504) at the transition (5004).

From the MT_Request_B message (202B), Home Network Authorizer (103) is able to gain the information about the identity of the terminal from the MT_ID field (304) in the step (6003). Using the identity, Home Network Authorizer (103) would retrieve the user's subscription information from its database or a backend server, e.g. HSS in 3GPP network. The Home Network Authorizer (103) would also parse the service request information obtained from the Service_Request field (305) in the step (6004). The service request could include various service specific information embedded, e.g. the bandwidth, delay, jitter, etc. Decision would be made in the Home Network Authorizer (103) using the user subscription information on whether to deny the service to the user in the step (6005). If the service requested is not supposed to be granted based on the user's subscription, the Home Network Authorizer (103) would set the flag to Deny of Service in the step (6013), and the state machine would transit to Service Reject state (504) at the taransion (5004). If the service is permitted, the Home Network Authorizer (103) would search its records for the terminal of the service for the session identifier, received in the Session_ID field (306) in the step (6007). If a record exists with the same session identifier, it means this is a handover request, and the terminal should be allocated the same address, so that the service session would

not be interrupted. If no record exists, it means it is a new request, and a record entry should be generated in the step (6008), and stored in the Home Network Authorizer (103)'s storage, or update the backend data base, e.g. the HSS. The Home Network Authorizer (103) would also identify the Service Provider Network (1003) using the service information, and a connection would be setup with the Service Provider Network Server (104).

From the Address_Request field (307), the Home Network Authorizer (103) obtains the address the Mobile Terminal (101) desires to use in the step (6009). If the Home Network Authorizer (103) does not wish to support this function due to operator policy or anything else, it can silently ignore this information. The Mobile Terminal (101) should always use the final address allocated from the Home Network Authorizer (103). The Home Network Authorizer (103) would decide from the service requested whether the address should be allocated locally or in the Home Network (1002), or in the Service Provider Network (1003). For example, if a user is only allowed to use the WLAN local service, the address should be allocated inside the WLAN, while for a user subscribed to a VPN service, it should be allocated with an address in that VPN.

The Home Network Authorizer (103) retrieves the tunnel type supported by the Mobile Terminal (101), from the Tunnel_Request field (308) in the step (6010). This information would be used to set up the tunnels for the service provisioning. The Mobile Terminal (101) could list out more than one tunnel type, and the first one in the list is the preferred type. The Home Network Authorizer (103) needs to check with the Service Provider Network Server (104), and decide which type to use. Extra information, for example direction of the tunnel, could also be included.

From the WLAN_ID field (309) , the Home Network Authorizer (103) would get the identity of the Wireless LAN that the Mobile Terminal (101) cur

rently is associated with in the step (6011). Using this information, th e Home Network Authorizer (103) would locate the corresponding WLAN Mana gement Server (102). This could be stored in the Home Network Authorizer (103)'s database as part of the roaming agreement, or be retrievable fr om the backend server, e.g. HSS. A secure link would be established afte r the server information is obtained. This link is used for the followin g service message signaling.

After obtained all the information, the Home Network Authorizer (103) would form the Service_Reqeust message (203), and the WLAN_Request,messa ge (205). This message would be sent out when the state machine of the H ome Network Authorizer (103) transits to the Wait State (504).

Figure 7 shows an example of the implementation of the Service_Request message (203). The message starts with the Home_Network_ID field (701). This field contains the information about the Mobile Terminal (101)'s h ome network identifier. It could be an operator's name, or a sub-system of a big network. The identifier should be globally unique. DNS name of the network, e.g. "network.operator.3gpp.org", is a good candidate for t his identifier. The presence of the home network information enables the Service Provider Network Server (104) to apply network policies, e.g. r oaming agreements, to the service request. The user profiles are managed by the Home Network (1002), and therefore the user information should n ot be sent to the Service Provider Network Server (104). However, to ena ble finer control of the service, user priority/grouping information cou ld be attached to the message. This could be concatenate with the home n etwork identifier, e.g. "goldmember.network.operator.3gpp.org". The Ser vice Provider Network Server (104) could use this to differentiate the u ser when granting services.

The next field is the MT_ID field (702). This field contains the infor mation about the Mobile Terminal (101)'s identifier. It is used by the H

ome Network Authorizer (103) for service tracking. The identifier could be the terminal's IMSI, or a temporary ID allocated by the Home Network Authorizer (103) specific for the service session. It should be consiste nt for the whole lifetime of the service session.

A Session_ID field (703) follows the above field. It is the session id entifier allocated by the terminal. The Service Provider Network Server (104) should keep a record of all the on-going session information. Ther efore, when the session identifier exists in the database, it means the service request is triggered by a handover, and therefore should use the same configurations to avoid service interruption. For example, when a session is active, the Service Provider Network Server (104) should allo cate the same address for the Mobile Terminal (101), so that the communi cation with the correspondence node can continue without any signaling.

The Address_Request field (704) is similar to that in the MT_Request_A message (202A). This part indicates to the Service Provider Network Ser ver (104) the type of address to allocate, e.g. IPv6. Similar to the Add ress_Requestfield (307) of the MT_Request_A message (202A), it also prov ides address requested by the Mobile Terminal (101). If the Service Prov ider Network Server (104) does not want to support this function, it cou ld ignore this information. If the Home Network Authorizer (103) decides the address needs not to be allocated from the Service Provider Network (1003), this field would be omitted.

The Service_Spec field (705) is a compound field. It contains the info rmation of the specific requirements from the Home Network Authorizer (1 03) based on the user's subscription. A possible implementation of this field (Data Structure 1) is shown below:

```
struct Service_Spec {
  u_long  bitrate_avg;
```

```
u_long  bitrate_max;
int  deliver_order;
int  MTU_size;
double  delay;
double  jitter;
int  priority;
int  service_direction;
int  QoS_type
struct timeval  start_time;
struct timeval  end_time;
};
```

Among the attributes, bitrate_avg and bitrate_max represent the guaranteed and maximum bit-rate for the service requested. The deliver_order attribute indicates whether the deliver is required to be in order. The MTU_size specifies the maximum data unit size to be transferred for the service. The delay and jitter fields specify some basic QoS attributes for the service. The priority attribute indicates the handling priority of the data traffic for this service. The service_direction attribute indicate whether the service is uni-directional, or bi-directional. The QoS_type attribute specifies the QoS schemes to be used for provisioning the service, e.g. DiffServ, or InterServ with RSVP, etc. The start_time, and end_time specify the starting and ending time of the service. The Service Provider Network Server (104) could use this information to schedule the resources for the service. It is obvious to anyone skilled in the art that other service specific attributes could be included in the structure in real implementation.

After the Service_Spec field (705) is the Tunnel_Spec field (706). This field contains the tunnel information, and is similar to the Tunnel_Request field (308) of the MT_Request_A message (202A), but with some extr

a information attached. For example, for the network tunnel entry, the W LAN end point is provided, and for the terminal tunnel, a security key c ould be attached for data encryption.

The last field of the Service_Request message (203) is the Security_Fi eld (707). This field is used to protect the whole message using the sec urity association between the Home Network Authorizer (103) and Service Provider Network Server (104). The exact algorithm used for this is impl ementation dependent.

It is obvious to anyone skilled in the art that the fields in the Serv ice_Request message (203) need not to be the described order. In real im plementation, the Home Network Authorizer (103) and Service Provider Net work Server (104) could negotiate any suitable order for the optimizatio n of signaling.

After the Service Provider Network Server (104) received the Service_R equest message (203), it would carry out the Service Address Management procedure (204). In this procedure, the Service Provider Network Server (104) would search its database for the session identifier contained in the Session_ID (703). If the session identifier for the same Mobile Term inal (101), exists Service Provider Network Server (104) copies all the information in its record, e.g. address of the MT, specification of the service, etc, and send that back to the Home Network Authorizer (103) as the reply message directly.

If the session identifier does not exist, the Service Provider Network Server (104) would create a new entry using the new session identifier as index in its database. The Service Provider Network Server (104) woul d check the Address_Request field (704), and allocate a suitable address for the Mobile Terminal (101) based on the address type specified in th is field.

The Service Provider Network Server (104) checks the Service_Spec fiel

d (705) from the Home Network Authorizer (103). If the requested service is not supported, a message indicates failure would be sent back to the Home Network Authorizer (103). Some error code could be used to specify the cause of the failure. If certain attributes in the Service_Spec fie ld (705) exceed the current capability of the Service Provider Network (1003), the Service Provider Network Server (104) would try to negotiate with the Home Network Authorizer (103) for a new set of attributes. This could be achieved by having the same Service_Request message (203) sent back to the Home Network Authorizer (103) with the Service_Spec field (705) modified to proposed value by the Service Provider Network Server (104).

The Service Provider Network Server (104) checks the Tunnel_Sepc field (706) for the matched tunnel type. There could be multiple matches, but the Service Provider Network Server (104) should choose the first match . For a Network Based Tunnel type, the Service Provider Network Server (104) needs to prepare the tunnel end points information in the reply mes sage. For the Client Based Tunnel, the Service Provider Network Server (104) would prepare tunnel type specific information, and include that in the reply information. For example, for a Mobile IPv6 type of scheme, t he Service Provider Network Server (104) needs to assign a Home Agent fo r the Mobile Terminal (101), and include possible some security informat ion in the reply message too. Directional information, e.g. uni-directio n, bi-direction, would also be attached to the tunnel information fields .

The Service Provider Network Server (104) replies to the Home Network Authorizer (103) with the Service_Reply message (205). The Service_Reply message (205) could use the same structure as the Service_Request messa ge (203) as shown in Figure 7. The contents of the Home_Network_ID field (701), MT_ID field (702), and Session_ID field (703) are copied directl

y from the corresponding Service_Request message (203). These fields would be used by the Home Network Authorizer (103) to match the request and reply message pair when the signaling link is reused for multiple terminals.

The content of the Address_Request field (704) in the Service_Reply message (205) contains the address(es) allocated to the Mobile Terminal (101). It could be a list of address entries with the first octet indicates the length of the field in byte. The following part of the field is the address list, with one octet indicating the address types followed by the actual address. Wildcard address is allowed. For example, if the address field is filled with all zero, it is indicating the Mobile Terminal (101) to form an address using WLAN local mechanisms, e.g. IPv6 auto-configuration [Non-patent document 17], or DHCP.

The content of the Service_Spec field (705) in the Service_Reply message (205) contains the attributes agreed by the Service Provider Network Server (104). It is identical to the Service_Spec field (705) in the corresponding Service_Request message (203), if all the attributes are approved by the Service Provider Network Server (104). Otherwise, it is the counter proposal of the Service Provider Network Server (104) to the Home Network Authorizer (103).

The Tunnel_Spec field (706) in the Service_Reply message (205)contains the tunnel setting chosen by the Service Provider Network Server (104). The exact content of this field is tunnel type specific. If a Client Based Tunnel type were chosen, only one setting is necessary. For example, if the Mobile IPv6 were agreed, the field would contain the address of the Home Agent assigned to the Mobile Terminal (101), and a security key for Binding Update authentication, etc. The address in the Address_Request field (704) would be used as the home address of the Mobile Terminal (101). If Network Based Tunnel type is chosen, the field would contain,

for example, the end-point address, and tunnel identifier, etc, and all the necessary details for each supported tunnel type.

In parallel with the Service_Request message (203), the Home Network Authorizer (103) would send a WLAN_Request message (206) to the WLAN Server (102). This message negotiates the necessary setting for provisioning service in the WLAN. An example of the implementation of this message is shown in Figure 8.

The WLAN_Request message (206) contains two fields, Home_Network_ID field (801) and MT_ID field (802) like the Service_Request message (203). The Home_Network_ID field (801) contains the identifier of the subscriber's home network. It is passed to the WLAN Server (102) in case some network policy would apply to the service provisioning. The MT_ID field (802) is used to track the location of the Mobile Terminal (101). It could be, for example, the Access Point identifier concatenated with the Mobile Terminal (101)'s lower layer identifier, e.g. MAC address.

The Address_Alloc field (803) is a flag to indicate whether a WLAN local address needs to be allocated for the Mobile Terminal (101), and the address types to be used. The Home Network Authorizer (103) would decide whether the local address is necessary based on the tunnel scheme chosen. In the example implementation, the first octet of this field indicates whether allocation is necessary with the following definition:

No_Allocation ::= 0x00;

Single_Stack_IPv4 ::= 0x01;

Single_Stack_IPv6_FullAddress ::= 0x02;

Single_Stack_IPv6_Prefix ::=0x03;

Dual_Stack_IPv4_Preferred ::= 0x04;

Dual_Stack_IPv6_Preferred_FullAddress ::= 0x05;

Dual_Stack_IPv6_Preferred_Prefix ::=0x06

It is obvious to anyone skilled in the art that other values could be

used in the real implementation of this message.

The Service_Support field (804) is a compound field that includes all the necessary attributes to support the service provisioning in the WLAN . The actual content is service specific. An example of the content of t his field is as that described in Data Structure 1.

The Tunnel_Setup field (805) is also a compound field. It uses the sim ilar format as the Tunnel_Spec field (706) in the Service_Request messag e (203).

The last field of the WLAN_Request message (206) is the Security_Field (806). This field is using the security association to protect the inte grity of the whole message. Algorithm used for the computation of this f ield is implementation dependent.

The WLAN Server (102) would carry out the WLAN Service Address Managem ent (207), after receiving the WLAN_Request message (206). For example, if the local IPv6 address allocation were requested by the Home Network Authorizer (103), the WLAN Server (102) would locate the suitable networ k section and allocate the IPv6 address for the terminal. If necessary, the WLAN Server (102) would also update the gateway, or firewall of the WLAN of the new address allocation, so that the Mobile Terminal (101) is able to access the service using this allocated local address.

The WLAN Server (102) would also use the information in the Service_Su pport field (804) to perform local admission control. Similar to the Ser vice Provider Network Server (104), if certain attributes exceeds the WL AN's current capacity, the WLAN Server (102) would try to negotiate a ne w set of service specification with the Home Network Authorizer (103), e .g. reduce the bit rate, change the service time interval, etc.

If a Client Based Tunnel scheme is chosen by the Home Network Authoriz er (103), the WLAN Server (102) does not need do any special setup. When the Network Based Tunnel scheme is used, the WLAN Server (102) needs to

identify the tunnel end points using the information from the MT_ID fie ld (802) .

The WLAN Server (102) replies the WLAN_Request message (206) with the WLAN_Reply message (208). The WLAN_Reply message (208) uses the similar structure as the WLAN_Request message (206) as shown in Figure 8. The Ho me_Network_ID field (801) and MT_ID field (802) are copied directly from the corresponding WLAN_Request message (206). These fields are used by the Home Network Authorizer (103) to match the request and reply messag e pair.

The Address_Alloc field (803) in the WLAN_Reply message (208) contains the information of the WLAN local address allocated to the Mobile Termi nal (101). The first octet of the field indicates the type of the addres s, as defined for Address_Request field (307) in MT_Request_A message (2 02A). The following part of the field contains the actual address alloca ted for the Mobile Terminal (101). For example, if a IPv6 address is all ocated, the first octet would be 0x02, and the next 32 octets contains t he actual IPv6 address.

The Service_Support field (804) in the WLAN_Reply message (208) contai ns the information of the service attributes as defined for the WLAN_Req uest message (206). If these service attributes were acceptable by the W LAN, the WLAN Server (102) would copy them directly from WLAN_Request me ssage (206). If the WLAN Server (102) could not agree on the attributes, it would send a new proposal in the WLAN_Reply message (208) with attri butes set to new values.

The Tunnel_Setup field (805) in the WLAN_Reply message (208) is the t unnel information for the Mobile Terminal (101). It specifies the tunnel type to be used in the first octet, and the tunnel type specific data i n the following octets. For example, if Mobile IPv6 is used for the data traffic, only tunnel type present in this field, and address in the Add

ress_Alloc field (803) would be used as the care-of-address of the Mobil e Terminal (101). If Mobile IPv4 is used, this field would contain the t unnel type in the first octet followed by the Foreign Agent address allo cated to the Mobile Terminal (101).

The Home Network Authorizer (103) would consolidate the information fr om the WLAN Server (102) and the Service Provider Network Server (104) a fter received the Service_Reply message (205) and WLAN_Reply message (20 8) . If the Service_Spec field (705) or Service_Support field (706) cont ains different attribute values than that in the Service_Request message (203) or WLAN_Request message (206), re-negotiation of service specific ation is necessary. The Home Network Authorizer (103) would check the ne w values proposed by the Service Provider Network Server (104) or the WL AN Server (102). If these new values were acceptable, it would confirm t he new setting using the SPN_Config message (210), and WLAN_Config messa ge (211).

The message pairs Service_Request message (203), Service_Reply message (205) and WLAN_Request message (206), WLAN_Reply messagge (208) do not have time correlation. They could happen in parallel, or one after anoth er depending on the implementation of the Home Network Authorizer (103). For example, the Home Network Authorizer (103) could decide to send out the WLAN_Request message (206) instead of Service_Request message (203) if the connection with the WLAN Server (102) is idle.

The SPN_Config message (210) is sent by the Home Network Authorizer (1 03) to the Service Provider Network Server (104) to confirm the new serv ice parameters if a re-negotiation is needed. Same message format as the Service_Request message (203) is used for the SPN_Config message (210). Some fields, e.g. the Address_Request would be omitted if not used.

Tunneling information could also be attached if necessary. For example , when Client Based Tunnel, e.g. Mobile IP, is used, the care-of-address

of the Mobile Terminal (101) allocated by the WLAN Server (102) would be inserted to the Tunnel_Request field (308). If a Network Based Tunnel is used, the tunnel end-point address, port number, etc, of the WLAN would be forwarded in this message.

The WLAN_Config message (211) serves the similar purpose. The Home Network Authorizer (103) uses this message to confirm new settings with the WLAN Server (102) if necessary. The message could also be used for forwarding tunnel information. For example, when the Network Based Tunnel is used, the tunnel end point address, port number, etc, of the Service Provider Network (1003) would be forwarded to the WLAN Server (102) in this message. WLAN Server (102) would then instruct the corresponding nodes to set up the tunnel. When the Client Based Tunnel is used, the terminal address would be included in the message, so that the WLAN could open the firewall for the data traffic.

It is obvious to anyone skilled in the art that these two messages, SPN_Config message (210) and WLAN_Config message (211) could be used by the Home Network Authorizer (103) to revoke the resources allocated for the Mobile Terminal (101) when the service session is over. For example, when the Home Network Authorizer (103) detected that the Mobile Terminal (101) is no longer in the WLAN, it would issue a WLAN_Config message (211) with Service_Support field (804) set to all zero. After received this kind of message, WLAN Server (102) would free all the resources allocated to the Mobile Terminal (101), and perform other appropriate actions.

The Home Network Authorizer (103) would send an MT_Reply_B message (212B) as the reply to the MT_Request_B message (202B). This message would be forwarded by the Access Point (105), or any other attendant, to the Mobile Terminal (101) as message MT_Reply_A message (212A). The MT_Reply_A message (212A) and MT_Reply_B message (212B) have the identical contents and format. Network Elements between the Home Network Authorizer (103

) and Mobile Terminal (101) has no access to the contents of these messa ges, and the Access Point (105) would only re-encapsulate the whole mess age and forward it. The MT_Reply_A message (212A) or MT_Reply B message (212B) is encrypted with the security association shared between the Mob ile Terminal (101) and Home Network Authorizer (103). Since the MT_Reply _A message (212A) is the reply to the corresponding MT_Request_A message (202A), the Access Point (105) would know which Mobile Terminal (101) t o forward.

If the WLAN Server (102) is on the path of the MT_Reply_B_message (212 B), the WLAN_Config message (211) could be piggybacked to the same messa ge. For example, if the WLAN Server (102) were the AAA server using Diam eter in the WLAN that would forwards the MT_Reply_B message (212B) to th e Mobile Terminal (101), the MT_Reply_B message (212B) could be encapsul ated in the Diameter-EAP-Answer AVP, while WLAN_Config message (211) bei ng encapsulated in another AVP in the same message. It is obvious to any one skilled in the art that same kind of scheme could be used even other transportation protocol is utilized.

The MT_Reply_A message (212A) has the same structure as the MT_Request _A message (202A), as shown in Figure 3. The Message_Type field (301) ha s the same format as that of the MT_Request_A message (202A). It would u se an integer to indicate that this message is a Reply instead of Reques t. The Message_Length field (302) indicates the total length of the mess age including the Message_Type field (301). The Domain_Name field (303) and the MT_ID field (304) in the MT_Reply_A message (212A) are the same as those in the MT_Request_A message (202A) . It is obvious to anyone sk illed in the art that these fields could be omitted in the real implemen tation for signaling optimization.

The Service_Request field (305) in the MT_Reply_A message (212A) is us ed to contain the service specific information set by the Home Network A

uthorizer (103) based on the user's subscription. For example, if a user requested for the IMS service, this could be the P-CSCF address. It is obvious to anyone skilled in the art that other information necessary to the service provisioning could be included in this field. The exact for mat of this field is service dependent.

The Session_ID field (306) in the MT_Reply_A message (212A) is copied directly from the MT_Request_A message (202A). It could be omitted in th e real implementation if not required by the Mobile Terminal (101).

The Address_Request field (307) in the MT_Reply_A message (212A) conta ins the address allocated to the Mobile Terminal (101). It should be use d by the service application as the source address. First octet of this field is the address type, and followed by the actual address. For examp le, if an IPv6 address prefix were allocated, the first octet would be 0 x03, and the following 32 octets contains the prefix information to be u sed by the Mobile Terminal (101) to form the actual IPv6 address. Other address information, e.g. WLAN gateway address, DNS server address, coul d also be included. These attributes would follow the address informatio n described above. Wildcard value of all zero indicates that the Mobile Terminal (101) should use local stateless mechanism to obtain the actual information.

The Tunnel_Request field (308) in the MT_Reply_A message (212A) contai ns the tunneling setting for accessing the service requested by the Mobi le Terminal (101). It would be tunnel type dependent. The first octet of this field indicates the tunnel types used.

For example, if Client Based Tunnel type Mobile IPv6 were used, the va lue would be 0x06, as defined for the tunnel types in the MT_Request_A m essage (202A). Following the type attribute, there would be the care-of-address allocated by the WLAN, and the Home Agent address, and the secur ity keys if necessary. The address in the Address_Request field (307) wo

uld be the Home Address allocated to the terminal.

If a Network Based Tunnel type were used, following the type attribute , there would be the address of the local end-point of the tunnel, and t he security keys for the Mobile Terminal (101) to securely communicate w ith the end-point.

The WLAN_ID field (309) in the MT_Reply_A message (212A) is copied dir ectly from the MT_Request_A message (202A). It could be omitted in real implementation for optimization of the signaling.

The Security_Field (310) of the MT_Reply_A message (212A) is used for protecting the integrity of the whole message. It uses the security asso ciation between the Mobile Terminal (101) and Home Network Authorizer (1 03). It should use the same algorithm as that for the MT_Request_A messa ge (202A).

After receiving the MT_Reply_A message (212A), the Mobile Terminal (10 1) would retrieve all the necessary information, and configure according ly. The Mobile Terminal (101) could start the actual service session (21 3) using the setting.

In real implementation, a Mobile Terminal (101) could request for a fe w service at the same time, e.g. a Voice-over-IP session together with a video streaming session. This would involve different Service Provider Network in the signaling. Same mechanism and message structure described above could be used in the scenario by aggregating several service requ ests in the same message. For example, in the MT_Request_A message (202A), there could be multiple sets of Service_Request field (305), Session_ ID field (306), Address_Request field (307), and Tunnel_Request field (308). These four fields would be grouped, and for each service requested by the Mobile Terminal (101), one group of these four fields would be i ncluded. For example, a MT_Request_A message (202A) requesting for a voi ce-over-IP session and a video streaming session, two groups of the list

ed four fields would present.

After receiving the MT_Request_B message (202B) that contains the same contents as the MT_Request_A message (202A), the Home Network Authorizer (103) would retrieve information from each set of these four fields corresponding to one specific service requested by the Mobile Terminal (101). Home Network Authorizer (103) would perform signaling for each of the requested services as described above for the single service request. For example, the Home Network Authorizer (103) would send Service_Request message (203) to both the IMS sub-system, and the network provides the streaming service. While for the WLAN_Request messages (206) for different services, they are destined for the same WLAN. The Home Network Authorizer (103) could be aggregate the information, and send only one message. If multiple WLAN_Request messages (206) need to be sent to the same WLAN, only one of them needs to request for the local address allocation .

The Home Network Authorizer (103) would aggregate all the service information into one MT_Reply_B message (212B) according to the order of the service requested, and forward that to the Mobile Terminal (101) through the Access Point (105). Mobile Terminal (101) could then configure itself using the information in the aggregated MT_Reply_A message (212A).

If the Mobile Terminal (101) requested multiple services in parallel, it is possible that different addresses are allocated to the terminal from different Service Provider Networks. It is also possible that different tunnels are setup for different service sessions. In this scenario, a special mid-layer processor is required. The service session identifier, as used in the Session_ID field (306) would be used by the mid-layer processor to multiplexing the address and tunnel setting.

The mid-layer processor in the Mobile Terminal (101) would maintain a local database of the address and tunnel information for different servi

ce sessions. When a service session is generated at the Mobile Terminal (101), the mid-layer processor would create an identifier for it. This is the session identifier that would be used in the Session_ID field (306) of the MT_Request_A message (202A). After received the MT_Reply_A message (212A) that contains all the address and tunnel information, the mid-layer processor would create a new entry in its database contains all the information indexed by the session identifier. When a service application needs to initiate a new connection session, it sends the request with the session identifier to the mid-layer processor. The mid-layer processor would retrieve corresponding address and tunnel information from its database using the session identifier. The address and tunnel information would be used by the normal stack, e.g. IP layer, to create suitable binding, e.g. socket, for the connection.

It is obvious to anyone skilled in the art that in real implementation, there could be WLAN that has no controller, i.e. no WLAN Server (102). In this case, the Mobile Terminal (101) has to use those WLAN local mechanisms for address allocation and tunnel setup. The Home Network Authorizer (103) would set the Address_Request field (307) and Tunnel_Request field (308) in the MT_Reply_A message (212A) to all zero, this would force the Mobile Terminal (101) to use WLAN mechanism, e.g. DHCPv6, MIPv6, etc, to configure the address.

In certain case, the Mobile Terminal (101) would desire to cancel the service registration in the WLAN. It is obvious to anyone skilled in the art that the above-described mechanism could also be used to de-register the service. The Mobile Terminal (101) could send out a MT_Request_A message (202A) with Service_Request field (305) set to a special value indicating the terminating of service. For example, the Service_Request field (305) could include a value as "terminate.request.IMS.foo.bar.operator-name.operator-group.gprs". The "terminate" before the "request" keyw

ord is the flag to terminate the service indicated by the APN attached after the "request" keyword. The Session_ID field (306) of the MT_Request_A message (202A) would be set to the session identifier of the service to be terminated. The Address_Request field (307) and Tunnel_Request field (308) could be omitted for this type of MT_Request_A message.

The Home Network Authorizer (103) would process the MT_Request_A message (202A) as normal. When it found the "terminate" keyword in the Service_Request field (305), it would retrieve the service session identifier from the Session_ID field (306). The Home Network Authorizer (103) would search its database for the session entry created at service registration time. This session entry would store the information about the settings of the service, e.g. the address allocated, the tunnel setting, etc. Using the information, the Home Network Authorizer (103) would send Service_Request message (203) to the Service Provider Network Server (104), and WLAN_Request message (206) to the WLAN Server (102) as normal. In these message, the Service_Spec field (705), and Service_Support field (804) are set to all zero.

The Service Provider Network Server (104), and WLAN Server (102), would process the message as normal. When they read the all zero Service_Spec field (705), or Service_Support field (804), they would know it is a service termination request. These two servers would search their database for the service session entry created at the service registration time, and free corresponding resources, e.g. the IP address, reserved bandwidth, etc, for the service session.

A MT_Reply_A message (212A) would be sent back to the Mobile Terminal (101), after the Home Network Authorizer (103) received notification from Service Provider Network (1003) and the WLAN. This message is to notify the success terminating of the service, and free of the reserved resources. In this MT_Reply_A message (212A), the Service_Request field (305)

contains the information about the result. For example, following value could be used in this field, "removed.request.IMS.foo.bar.operator-name.operator-group.gprs", where the "removed" keyword before the "request" keyword indicates the success deregistration of the service. It is obvious to anyone skilled in the art that extra information could be included, e.g. appended after the "removed" keyword.

In the process of provisioning service to the Mobile Terminal (101), policy control would involve. For example, a terminal using its GPRS interface is allowed 149Kbps access rate. When this terminal roamed into a WLAN, it transits to use its WLAN interface for accessing the same service. Since the WLAN provides much higher air interface bandwidth, the terminal is expected to enjoy higher access rate, e.g. 1 Mbps. In order to achieve this higher service rate to the Mobile Terminal (101), policy control framework needs to be invoked to modify corresponding policy settings, e.g. gateway filters. In the above example, the control point, e.g. the GGSN would only reserve 149Kbps bandwidth for the terminal's service when it initiates the service using the GPRS interface. When the Mobile Terminal (101) registers the service session again using the WLAN service, the policy server should modify the settings at the GGSN to the 1Mbps. It is obvious to anyone skilled in that art that other kind of setting, and control node would be involved in the policy control.

This kind of policy control should based on the user's subscription, and therefore in the Home Network domain. The present invention uses the Home Network Authorizer (103) to handle the service request and address, tunnel setup. Therefore, it has all the necessary information for the policy control decision. This information could be passed by the Home Network Authorizer (103) to the Policy Server of the Home Network domain. The Policy Server could in turn use the policy control interface to manipulate the corresponding node, e.g. the GGSN, to act accordingly. The Pol

icy Server could also inform other networks involved in the service provisioning using the policy control framework. For example, the Policy Server in the Home Network domain could inform the Policy Server in the WLAN of the new access rate limit, so that the WLAN Policy Server could adjust local admission control mechanism accordingly.

Figure 9 shows an example implementation of the message used between the Home Network Authorizer (103) and the Policy Server. The message starts with the Operation field (901). This field indicates the operation to be taken by the Policy Server. Possible value could be:

Install ::= 0x01;

Remove ::= 0x02;

Update ::= 0x03;

When Home Network Authorizer (103) received a new service session request from the Mobile Terminal (101), it would use value "Install" in the Operation field (901). When the Mobile Terminal (101) terminates a service session, the Home Network Authorizer (103) would use "Remove" value in the Operation field (901). The "Update" value would be used when the service request from the Mobile Terminal (101) is regarding an active service session. It is obvious to anyone skilled in the art that other types of value could be used in real implementation.

Second field is the MT_ID field (902). This field contains the identifier of the Mobile Terminal (101). For example, it could be the IMSI of the mobile user.

Third field is the MT_Location field (903). This field would be used by the Policy Server to retrieve location based service policy, e.g. provide double access rate when the terminal is certain WLAN. This field could contain, for example, the WLAN identifier from the WLAN_ID field (309) in the MT_Request_A message(202A).

The next field is the MT_Service field (904). This field indicates wha

t kind of service is access by the Mobile Terminal (101). It could also contain the service session information. An example of the content in th is field could be the APN plus the session identifier.

The next field is the Tunnel_Setting field (905). This field indicates the tunnel setting used by the Mobile Terminal (101) in the WLAN. The c ontents of this field are the tunnel type followed the tunnel end point address, port number, etc. The exact format is tunnel type specific. The tunnel type used is as those defined for the Tunnel_Request field (308) in the MT_Request_A message (202A).

The last field of the message is the MT_Address field (906). This fiel d contains the address used by the Mobile Terminal (101) in the WLAN. Th is could be used by the Policy Server to set the filtering rules for acc essing the service.

It is obvious to anyone skilled in the art that in real implementation , the message fields need not follow the exact order as described above. Each field could also include extra information not described in the ex ample in actual implementation.

Effects of Invention

The present invention provides a way for managing the address allocati on of the terminal in WLAN inter-working. When it deployed, the mobile t erminal could be allocated an address based on the service it requested and its subscription information. The address management could be carrie d out without requiring access to the local resources. The invention als o provides a method for control the tunnel setup in the WLAN interworkin g. With it, the mobile terminal could support either network based or cl ient based tunnel setup together with the service authorization. This in vention also provides a method for interworking with the policy control framework. Using the interface provided, the service authorization, addr

ess allocation, and tunnel setting information could be propagated to th e policy servers, and proper action could be taken to better deliver the service to the terminal. With all the methods, the address management, tunnel setup, and service authorization could be accomplished within one roundtrip message exchange the terminal and its home domain server. Thu s, precious signalling time, and bandwidth could be saved.

4　Brief Description of Drawings

Figure 1 is a block diagram showing an example of the network structur e that is used by the invention for managing the address allocation, tun nelling setup, and service negotiation for the mobile terminal in the WL AN interworking;

Figure 2 is a sequence chart showing an example of the message sequenc e that used by the architecture shown in Figure 1 for the terminal addre ss allocation, tunnelling setup, and service negotiation;

Figure 3 is a data structure view showing the structure of an example implementation of the message used by the mobile terminal in the message exchanges shown in Figure 2;

Figure 4 is a data structure view showing an example format that could be used by the mobile terminal for the address allocation request;

Figure 5 is a state chart showing an example implementation of the Hom e Network Authorizer in the framework shown in Figure 1 for mobile termi nal address allocation, tunnelling setup, and service negotiation in WLA N interworking;

Figure 6 is a flow chart showing an example flow chart that could be u sed for implementation of the request message processing procedure at th e Home Network Authorizer;

Figure 7is a data structure view showing the structure of an example i mplementation of the message used by the Home Network Authorizer to nego

tiating mobile terminal service specification, address allocation, and t unnel settings with Service Provider Network Server;

Figure 8 is a data structure view showing the structure of an example implementation of the message used by the Home Network Authorizer to neg otiating mobile terminal service specification, address allocation, and tunnel settings with WLAN Server;

Figure 9 is a data structure view showing the structure of an example implementation of the message used by the Home Network Authorizer to upd ate the policy server in the Home Network domain of the Mobile Terminal' s status.

Description of the Symbols

101 Mobile Terminal (MT)

102 WLAN Management Server (WLAN Server)

103 Home Network Authorizer

104 Service Provider Network Management Server (Service Provider Netwo rk Server)

105 Access Point

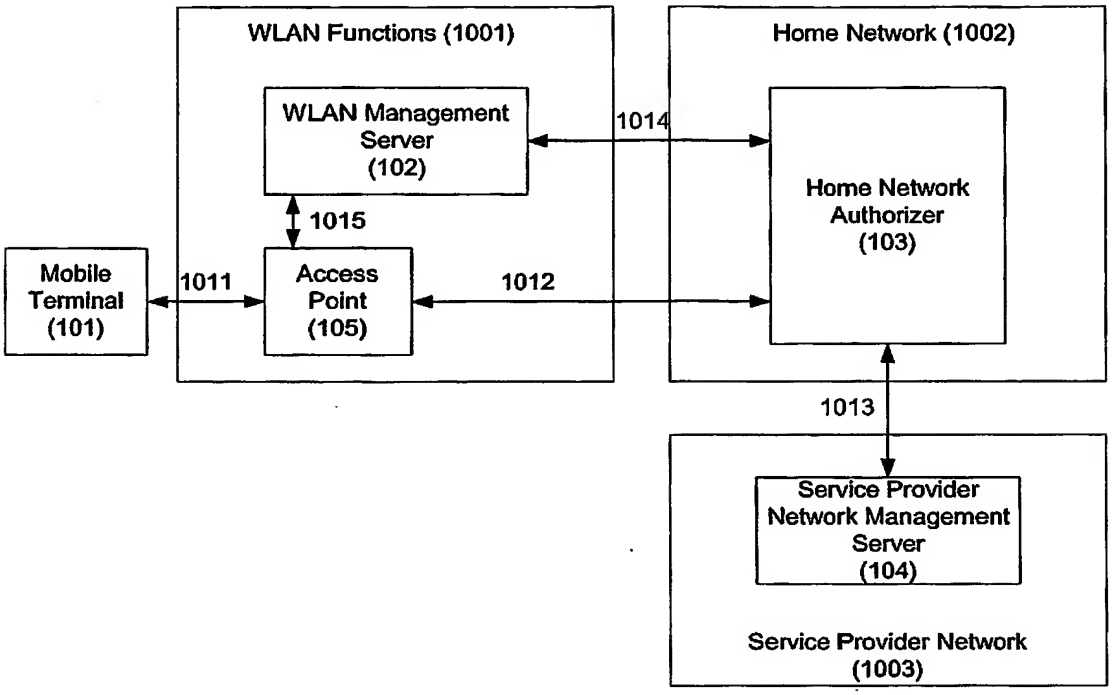
1001 WLAN Functions

1002 Home Network

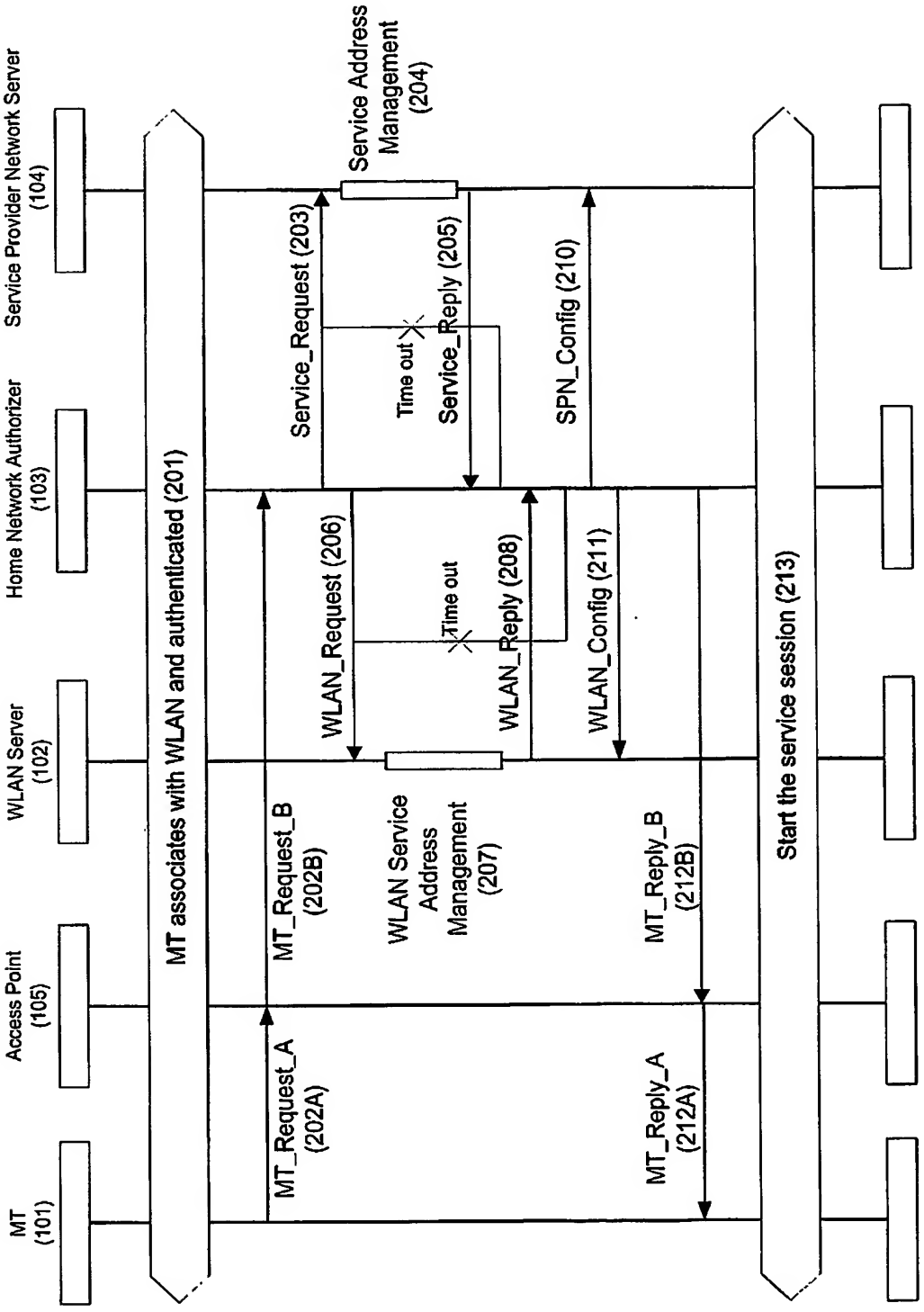
1003 Service Provider Network

【書類名】　外国語図面

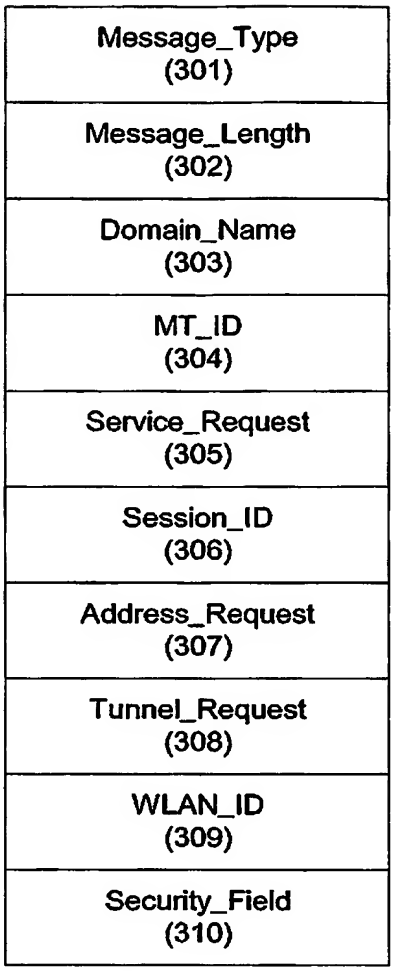
【図１】


WLAN Functions (1001)
Home Network (1002)
WLAN Management Server (102)
1014
Home Network Authorizer (103)
1015
Mobile Terminal (101)
1011
Access Point (105)
1012
1013
Service Provider Network Management Server (104)
Service Provider Network (1003)

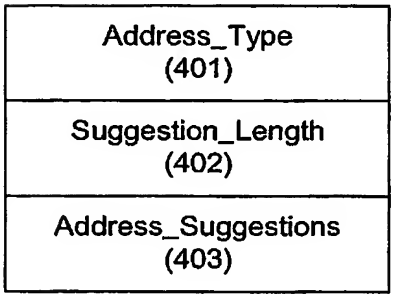
【図２】


MT (101)
Access Point (105)
WLAN Server (102)
Home Network Authorizer (103)
Service Provider Network Server (104)
Service Address Management (204)
MT associates with WLAN and authenticated (201)
MT_Request_A (202A)
MT_Request_B (202B)
Service_Request (203)
Time out
Service_Reply (205)
WLAN_Request (206)
WLAN Service Address Management (207)
Time out
WLAN_Reply (208)
SPN_Config (210)
WLAN_Config (211)
MT_Reply_A (212A)
MT_Reply_B (212B)
Start the service session (213)

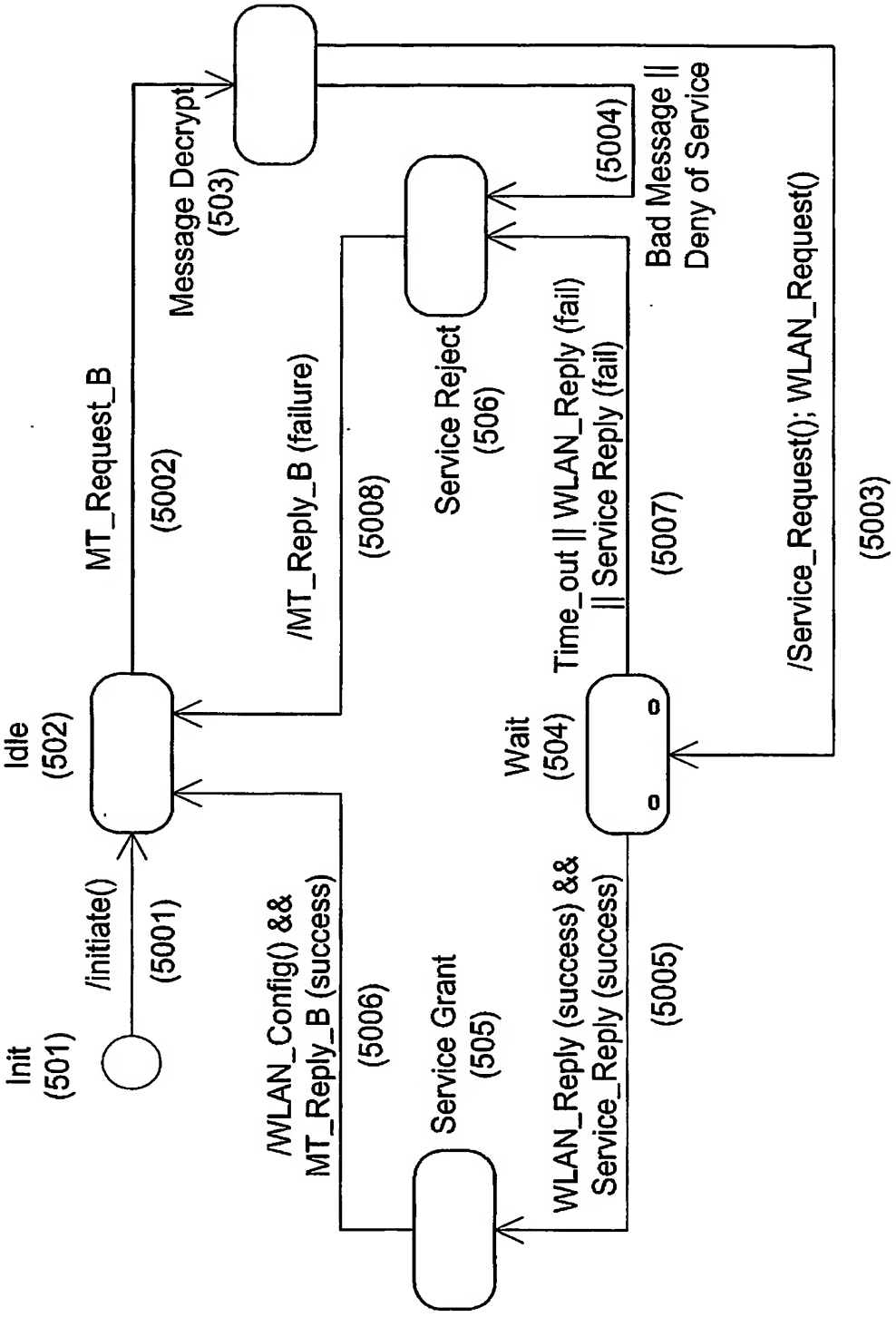
【図３】


Message_Type
(301)
Message_Length
(302)
Domain_Name
(303)
MT_ID
(304)
Service_Request
(305)
Session_ID
(306)
Address_Request
(307)
Tunnel_Request
(308)
WLAN_ID
(309)
Security_Field
(310)

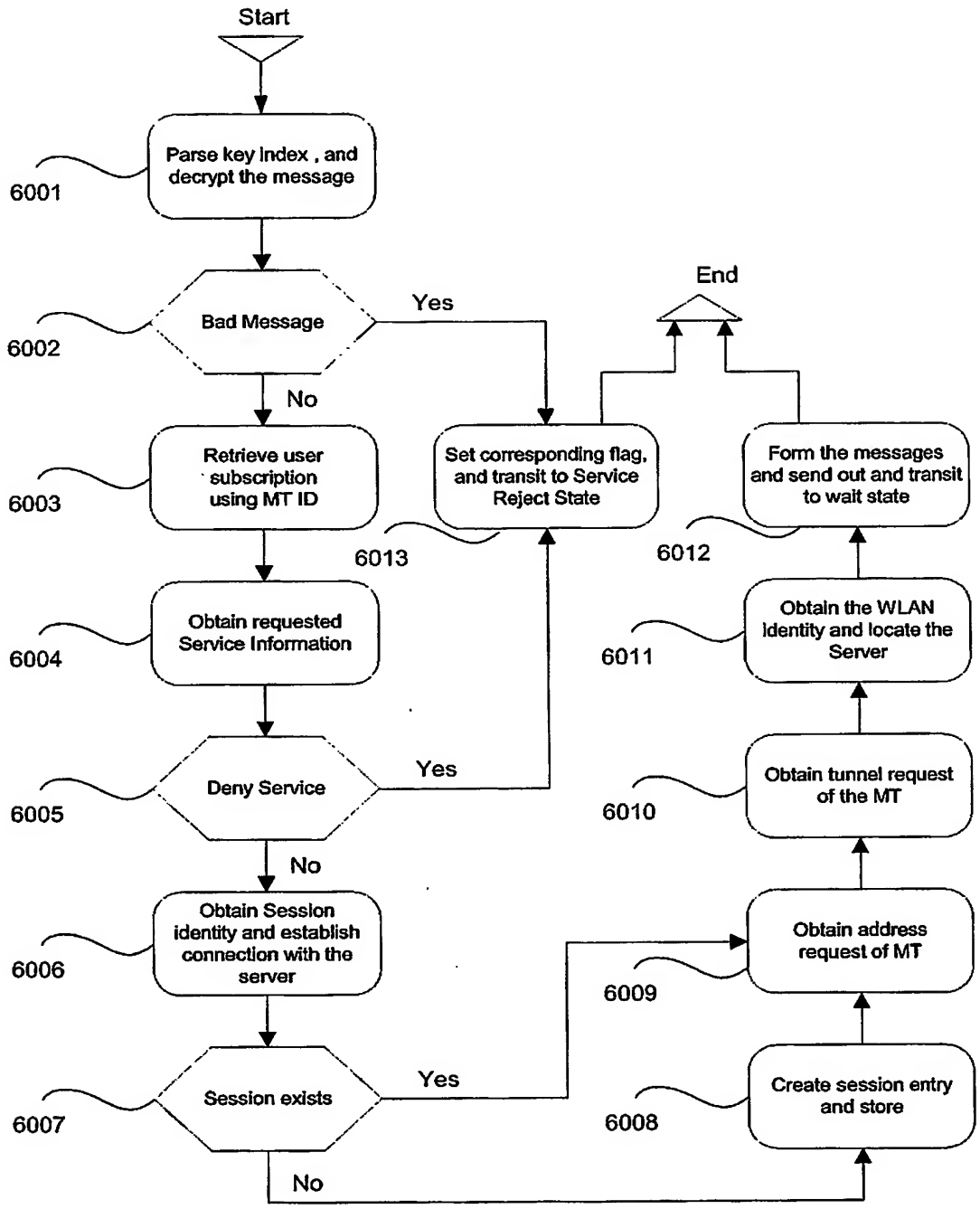
【図４】


Address_Type
(401)
Suggestion_Length
(402)
Address_Suggestions
(403)

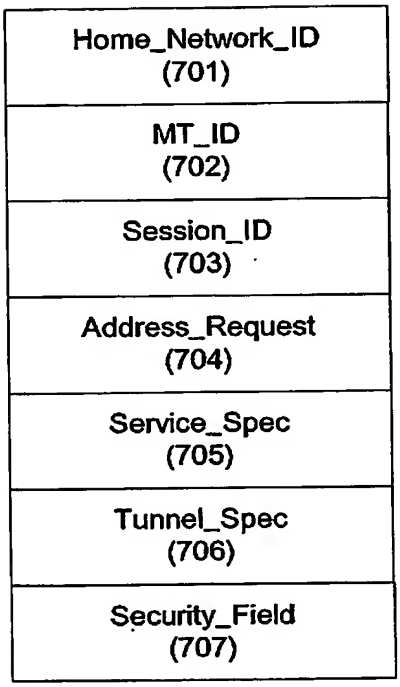
【図５】


Init
(501)
/initiate()
(5001)
Idle
(502)
MT_Request_B
(5002)
Message Decrypt
(503)
/WLAN_Config() &&
MT_Reply_B (success)
(5006)
Service Grant
(505)
WLAN_Reply (success) &&
Service_Reply (success)
(5005)
Wait
(504)
Time_out || WLAN_Reply (fail)
|| Service Reply (fail)
(5007)
/MT_Reply_B (failure)
(5008)
Service Reject
(506)
Bad Message ||
Deny of Service
(5004)
/Service_Request(); WLAN_Request()
(5003)

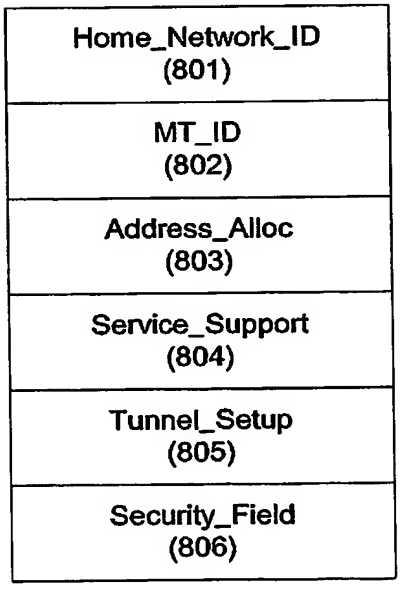
【図６】


Start
Parse key Index , and decrypt the message
6001
Bad Message
Yes
6002
No
Retrieve user subscription using MT ID
6003
Set corresponding flag, and transit to Service Reject State
6013
End
Form the messages and send out and transit to wait state
6012
Obtain requested Service Information
6004
Obtain the WLAN Identity and locate the Server
6011
Deny Service
Yes
6005
Obtain tunnel request of the MT
6010
No
Obtain Session identity and establish connection with the server
6006
Obtain address request of MT
6009
Session exists
Yes
6007
Create session entry and store
6008
No

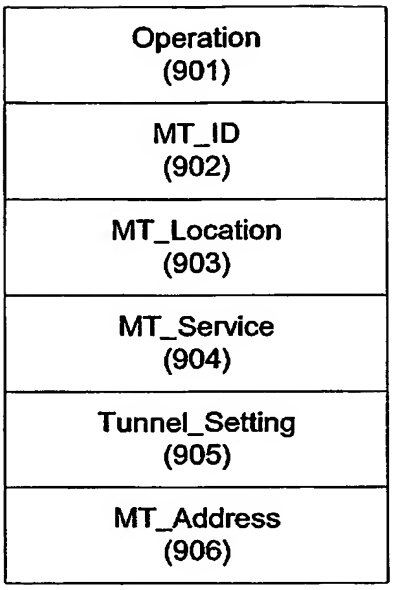
【図７】


Home_Network_ID
(701)
MT_ID
(702)
Session_ID
(703)
Address_Request
(704)
Service_Spec
(705)
Tunnel_Spec
(706)
Security_Field
(707)

【図８】


Home_Network_ID
(801)
MT_ID
(802)
Address_Alloc
(803)
Service_Support
(804)
Tunnel_Setup
(805)
Security_Field
(806)

【図９】


Operation
(901)
MT_ID
(902)
MT_Location
(903)
MT_Service
(904)
Tunnel_Setting
(905)
MT_Address
(906)

【書類名】　外国語要約書

1　ABSTRACT

The present invention provides a solution to the mobile terminal address management in the WLAN interworking. By using the access control framework, the mobile terminal could obtain the address, and setup the tunnel together with the granting of service access. The management process would be shielded by the inherent encryption and protection of the access control process, and thus does not need extra security setup procedures to be performed. The invention also provides a method for the terminal to obtain address that binds to the session, using a fine grain service authorization procedure. The terminal could maintain multiple addresses when accessing multiple parallel sessions. The address management is also integrated with the policy control mechanisms. The policy control would provide means for the terminal and its home network to configure the WLAN when necessary after an address alternation. QoS, or tunnelling information would be modified and provisioned accordingly to the new status using channels available in the existing policy control procedures. By this, a smooth address transition in the roaming time could be achieved, and QoS interruption could be minimised.

2　Representative Drawings　Fig. 2

認定・付加情報

特許出願の番号	特願２００３－００６１７５
受付番号	５０３０００４６７７５
書類名	特許願
担当官	末武　実　　１９１２
作成日	平成１５年　３月１９日

＜認定情報・付加情報＞

【提出日】　平成15年 1月14日

次頁無

特願２００３－００６１７５

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社